



WEB SITE SELF ASSESSMENT CHECKLIST

Updated: 27 Mar 2014

- Ref A DODI 8550.01, September 11, 2012, DoD Internet Services and Internet-Based Capabilities
<http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf>
- Ref B SECNAVINST 5720.44C, 21Feb2012 - Department of the Navy Public Affairs Policy and Regulations (Chap 7)
<http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-700%20General%20External%20and%20Internal%20Relations%20Services/5720.44c.pdf>
- Ref C SECDEF Memo 28DEC2001- Removal of Personally Identifying Information of DoD Personnel from Unclassified Web Sites
http://www.public.navy.mil/fcc-c10f/niocnorfolk/Documents/names_removal.pdf
- Ref D SECDEF Memo 13JUL2000 - Privacy Policies and Data Collection on DOD Public Web Sites
http://www.public.navy.mil/fcc-c10f/niocnorfolk/Documents/SECDEF13JUL2000_cookies.html
- Ref E NTD 02-14, 261631Z MAR 14 (ALCOM 046-14) Policy and Procedures for Web Risk Assessment (WRA) of Unclassified Navy Websites
<http://www.public.navy.mil/fcc-c10f/niocnorfolk/Documents/NTD-08-09.txt>
- Ref F OMB Circular A-130 Management of Federal Information Resources
<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>
- Ref G NAVADMIN 145/07, 051353Z JUN 07, Consolidation of Navy Websites – Reduction of IM/IT Footprint
<http://www.public.navy.mil/fcc-c10f/niocnorfolk/Documents/NAV07145.txt>
- Ref H JTF-GNO CTO 08-012
<https://www.jtfgno.mil>
- Ref I Navy Imagery Decision Tree
http://www.public.navy.mil/fcc-c10f/niocnorfolk/Documents/navy_imagery_archiving_decision_tree_final.pdf
- Ref J OSD Memo 23NOV2010 – Social Security Numbers (SSN) Exposed on Public Facing and Open Government Websites
https://www.chinfo.navy.mil/socialmedia/OSD_memo_13798-10.pdf
- Ref K DoD Memo DTM-08-060 9MAY2008 with change 6SEP2011- Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement
<http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-060.pdf>
- Ref L NAVADMIN 178/11, 091848Z JUN 11, Suicide Prevention Quarterly Update
<http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMIN/NAV2011/NAV11178.txt>
- Ref M Federal Register: July 20, 2006 (Volume 71, Number 139), Rules and Regulations, Page 41095-41099, DOCID:fr20jy06-1
<http://edocket.access.gpo.gov/2006/E6-11541.htm>
- Ref N DODCIO Memo: 16JUL2013 – Office of Management and Budget (OMB) Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act of 1973
http://dodcio.defense.gov/Portals/0/Documents/Section%20508/Sec508%20memo_signed%2016Jul2013_compliant.pdf

This document contains a summary of website content requirements and restrictions for publicly accessible Navy websites. A website satisfies the definition of being “publicly accessible” if any of the content on the website is accessible by the public via anonymous access. Restricting access by domain validation [Ref B, Chap 7] or SSL without client-side authentication is not sufficient to be excluded from the definition of “publicly accessible”.

Authorized publicly accessible web presence:

- ❑ **No entity below the command level or its' equivalent is authorized to establish a publicly accessible web site.**

[Ref B, Chap 7]

Only commissioned units are authorized to register a domain name for a website. Non-commands are allowed to create a web presence but only as a sub-web off of an authorized web site. Sub-webs will appear as an integral part of their command level parent web site. For instance, sub-webs will be implemented with the same "theme" as the parent web site and any "home" buttons on the sub-web pages must link to the parent's web site home page only.

Navy publicly accessible web sites MUST:

- ❑ **Contain the Full command's organizational name and mailing address.**

[Ref B, Chap 7]

The full command organizational name (with no abbreviations) must be prominently displayed on the web site home page.

- ❑ **Contain the statement "This is an official U.S. Navy web site".**

[Ref B, Chap 7]

The exact phrase "This is an official U.S. Navy web site" (or U.S. Marine Corps) must be prominently displayed on the web site home page.

- ❑ **Contain a tailored Privacy Policy.**

[Ref B, Chap 7; Ref A Enclosure 3, figure 2]

The web site Privacy Policy or a hyperlink to the web site Privacy Policy must be prominently displayed on the web site home page.

The Privacy Policy **MUST BE** verbatim from Ref A. The only authorized modifications are to substitute the items indicated and to use Privacy Policy versus Privacy and Security Notice. (Note that reference(p) below is left intact here as it relates to the list of references in Ref A of this document.) Links to this tailed privacy policy must be labeled "Please read our Privacy Policy Notice." as per Ref B.

Privacy Policy example per Ref A:

Quote:

PRIVACY AND SECURITY NOTICE

1. [Name of service (e.g., "Website Title")] is provided as a public service by [name of the DoD Component(s)].
2. Information presented on this service not identified as protected by copyright is considered public information and may be distributed or copied. Use of appropriate byline, photo, and image credits is requested.
3. For site management, information is collected [Link "information is collected" to description of specific information. An example is provided after paragraph 8. in this figure] for statistical purposes. This U.S. Government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
4. For site security purposes and to ensure that this service remains available to all users, software programs are employed to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations and national security purposes, no other attempts are made to identify individual users or their usage habits beyond DoD websites. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines. [Agencies subject to Reference (o) shall add the following sentence to this paragraph: “All data collection activities are in strict accordance with DoD Directive 5240.01.”]
6. Web measurement and customization technologies (WMCT) may be used on this site to remember your online interactions, to conduct measurement and analysis of usage, or to customize your experience. The Department of Defense does not use the information associated with WMCT to track individual user activity on the Internet outside of Defense Department websites, nor does it share the data obtained through such technologies, without your explicit consent, with other departments or agencies. The Department of Defense does not keep a database of information obtained from the use of WMCT. [If the DoD CIO has provided explicit written approval to use Tier III WMCT, cite that approval here.] General instructions for how you may opt out of some of the most commonly used WMCT is available at http://www.usa.gov/optout_instructions.shtml.
7. Unauthorized attempts to upload information or change information on this site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act (18 U.S.C. § 1030).
8. If you have any questions or comments about the information presented here, please forward them to [contact information to report both technical and information problems with the website specifically, including accessibility problems].

❑ **Contain the Webmaster contact information.**

[Ref B, Chap 7]

Information on how to contact the Webmaster must be displayed on the web site home page or at least contained within the source code of the home page. Ideally Webmaster contact information should be listed on the web site home page and should include; an e-mail address, work telephone number, and work mailing address.

❑ **Contain a link to parent command or Immediate Superior in Command (ISIC).**

[Ref B, Chap 7]

Please label the link with the text “Parent Command”, “Immediate Superior in Command”, or “ISIC”. This link is required on the home page.

❑ **Contain a link to the official U.S. Navy web site: www.navy.mil.**

[Ref B, Chap 7]

This link is required on the home page.

❑ **Contain a link to Navy recruiting web site: www.navy.com.**

[Ref B, Chap 7]

This link is required on the home page.

❑ **Contain a link to Freedom of Information Act (FOIA) web site: www.foia.navy.mil or foia.navy.mil.**

[Ref B, Chap 7]

This link is required on the home page.

❑ **Contain a link to Suicide Prevention Lifeline web site: <http://www.suicidepreventionlifeline.org/Veterans/Default.aspx>.**

[Ref L, 3]

This link is required on the home page. Use the associated icon.

- ❑ **Contain a link to No Fear Act: for example link to http://www.opm.gov/about_opm/nofear/notice.asp or <http://www.public.navy.mil/donhr/Pages/NoFear.aspx>. [Ref M, Comments on Notification Obligations]**
This link is required on the home page.

- ❑ **External links to non U.S., state, or local government web sites must be accompanied by a disclaimer statement.**
[Ref A, Enclosure 3, and Ref B, Chap 7]
External links to non-government web sites that directly support the command's mission are authorized but a disclaimer statement must be displayed on the page or pages listing external links or through an intermediate "exit notice" page.
External link disclaimer notice Example:
"The appearance of hyperlinks does not constitute endorsement by the [insert sponsoring organization, i.e., Department of Defense, U.S. Army, U.S. Navy, U.S. Air Force, or U.S. Marine Corps] of non-U.S. Government sites or the information, products, or services contained therein. Although the [insert sponsoring organization] may or may not use these sites as additional distribution channels for Department of Defense information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this website."

- ❑ **Accompany all solicitations from the web site visitor with a Privacy Advisory.**
[Ref B, Chap 7; Ref A, Enclosure 3]
The term "solicitation" encompasses any and all requests for submissions including surveys, forms, and Webmaster feedback.
Privacy Advisory example:
"We will not obtain personally identifying information about you when you visit our site unless you choose to provide such information to us. If you choose to send email to the site webmaster or submit an online feedback form, any contact information that you provide will be solely used to respond to your request and not stored."

Per ref A:
The privacy advisory shall be posted on the web page where the information is being solicited or provided through a well-marked hyperlink. Providing the hyperlink via a statement, such as "Privacy Advisory: Please refer to the Privacy Policy that describes why this information is being collected and how it will be used," is satisfactory when linked directly to the applicable portion of the Privacy Policy

- ❑ **Have the written approval of SECDEF for the use of persistent cookies.**
[Ref A, Enclosure 3; Ref B, Chap 7]
Cookies that remain after a browser session is terminated are persistent cookies.

- ❑ **A Notice and Consent Banner.**
[Ref K, attach 1: A]
A verbatim Notice and Consent Banner (sometimes referred to as a DoD Warning Banner) must be prominently displayed at the access point for web sites where access is controlled by a level 3 Security and Access Control mechanism (i.e., User Authentication).
Notice and Consent Banner Example:
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or

services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

- ❑ **Ensure all photos have been assigned a Visual Information Record Identification Number (VIRIN) and are properly archived.**

[Ref I]

http://www.public.navy.mil/fcc-c10f/nioconorfolk/Documents/navy_imagery_archiving_decision_tree_final.pdf should be reviewed. Send VIRIN questions to navyvisualnews@navy.mil.

- ❑ **Assist the public in locating government information.**

[Ref F, 8.a.5.(d).(iv)]

Small sites may use site maps or indexes. Larger sites should implement their own search functionality. Note that this requirement can no longer be met by registering with the Government Information Locator Service (GILS) since GILS was discontinued Dec 2005. In addition, the Defense Technology Information Center (DTIC) has discontinued its site crawl support (i.e., www.dtic.mil/dtic/search/submit_site.html is no longer available). Sites may also register at <http://www.defense.gov/RegisteredSites/SubmitLink.aspx>.

- ❑ **Provide accessibility to all U.S. citizens, including persons with disabilities.**

[Ref B, Chap 7]

Visit <http://www.doncio.navy.mil/section508toolkit/sec0401webbasedaps.htm> for more information.

- ❑ **Register with the DON Application and Database Management System (DADMS).**

[Ref E and G]

Per NAVADMIN 145/07, all Navy websites must be registered with DADMS. Please see <https://www.dadms.navy.mil> for details. Note that the site is CAC/PKI enabled and also requires a user account. The DADMS Portal/Web site Registration Process Guide is available for those with DADMS accounts. DADMS Helpdesk Support: DADMS@att.com or call (703) 506-5220.

- ❑ SharePoint sites hosted by another command do not need to register with DADMS. In addition, a Navy site hosted by another DoD component does not need to register with DADMS (e.g., NIOC Colorado's site <http://www.buckley.af.mil/units/nioe>).

- ❑ **Websites must include a Section 508 link on the website**

[Ref N]

All Navy Internet and intranet sites must include an "Accessibility/Section 508" link in the footer, which links to the DoD statement on accessibility at http://dodcio.defense.gov/DoDSection508/Std_Stmt.aspx.

Navy publicly accessible web sites must NOT contain:

- ❑ **Overt warning signs or words of warning or danger in association with the Privacy Policy. The Privacy Policy can only be identified with the phrase “Privacy Policy”.**
[Ref A, Enclosure 3; Ref B, Chap 7]
Indicators that create a misperception of danger in association with the Privacy Policy will not be used. The Privacy Policy can only be identified with the phrase “Privacy Policy”. All references (links) to the Privacy Policy, including the required home page link, shall state: “Please read our Privacy Policy notice.”
- ❑ **Altered photos (other than standard photographic processes).**
[Ref B, Chap 7]
Some alterations are acceptable as long as the alterations do not defer from the original intent.
- ❑ **FOUO or above information.**
[Ref A, Appendix to Enclosure 3; Ref B, Chap 7]
- ❑ **Personally identifying content.**
[Ref A, Appendix to Enclosure 3; Ref B, Chap 7; Ref C]
Any information other than name, rank/rate, and duty station that can be used to identify DoD individuals. Exception: Command Executives (i.e., CO, XO, CMC) can be identified by photo and name only. The following table lists specific information that is not to be divulged.

Social Security Number*	Marital Status	Age
Home address or phone numbers**	Birth date	Personal email addresses
Race, religion, citizenship	Family members - except spouses of senior leadership participating in public events	

*To include last four **[Ref J]**.
** For personnel such as the command ombudsman, when a command issued cell phone and/or pager is not available, consider the use of a command number that can either be forwarded to the ombudsman’s personal phone or allow message retrieval.
- ❑ **Proprietary or copyrighted content.**
[Ref A, Appendix to Enclosure 3; Ref B, Chap 7]
- ❑ **Operational Lessons Learned.**
[Ref A, Appendix to Enclosure 31; Ref B, Chap 7]
- ❑ **Information revealing sensitive military operations, exercises, vulnerabilities, maps identifying command and operational facilities.**
[Ref A: Appendix to Enclosure 3; Ref B, Chap 7]
- ❑ **Information for specialized, internal audience or of questionable value to the general public.**
[Ref B, Chap 7]
Only content that is specifically targeted for the general public should be posted on web sites that have no access restrictions implemented. Content intended for an internal audience cannot be protected by domain restriction alone.
- ❑ **Information that places national security, personnel, assets, or mission effectiveness at unacceptable risk.**
[Ref A, Appendix to Enclosure 3; Ref B, Chap 7]

- ❑ **Phone numbers that can be associated with individuals. Only phone numbers for commonly requested resources and services or for office codes are allowed.**
[Ref C, Ref B, Chap 7]
 Exceptions include Public Affairs Officers, command spokes persons, primary care givers, and chaplains.
- ❑ **Product endorsements, preferential treatment of any private organization or product, or references including logo or text indicating that the site is “best viewed” with any specific web browsers.**
[Ref A, Enclosure 3; Ref B, Chap 7]
- ❑ **Contain links or references to documents within DoD Web sites that have security and access controls.**
[Ref A, Appendix to Enclosure 3; Ref B, Chap 7]
 However, it is permissible to link to log-on sites, provided details as to the controlled site’s contents are not revealed.
- ❑ **Content duplicated from other military web resources.**
[Ref B, Chap 7]
 Navy web sites may reference (via hyperlink) these external resources instead.
 For example you may provide a link to:
http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=900&ct=4 for ship characteristics for Destroyers or http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=200&ct=4 for Aircraft Carriers . Note that a ship may publish its own characteristics since the ship has release authority over the data.
- ❑ **Automatic posting of information submitted by unauthorized personnel.**
[Ref B, Chap 7]
 Web logs or blogs may not support automatic postings by unauthorized personnel.
- ❑ **Government Information Locator Service (GILS) ID or Number.**
[Ref B, Chap 7]
 The Government Information Locator Service (GILS) was discontinued Dec 2005. As a result, NIOC Norfolk no longer uploads registrations to GILS. Unfortunately when SECNAVINST 5720.47B was published in Dec 2005 it still contained the GILS requirement. The author has been notified and will remove the reference before the next release. Note that the service once provided by the Defense Technology and Information Center (DTIC) via http://www.dtic.mil/dtic/search/dod_search.html is also no longer available.
- ❑ **A Notice and Consent Banner.**
[Ref A, Enclosure 3]
 A Notice and Consent Banner (sometimes referred to as a DoD Warning Banner) must NOT be displayed on publicly accessible Navy web sites unless it is associated with an access point for a sub URL where access is controlled by a level 3 Security and Access Control mechanism (i.e., User Authentication).